Dr. David A. Honey
Director
Advanced Technology Office
The Network as Weapon

Network Centric Warfare:

- What is it?
- How does it work?
- Why should you care?

These are the questions that ATO will answer for you today, and in turn, show you why we believe that Network Centric Warfare is the key to DoD achieving rapid, pervasive, and sustained dominance in future military operations.

All too often, the Network Centric Warfare story focuses on things like routers, switches, and communications links. This is a platform centric view that misses the real point!

Network Centric Warfare is not about sticking commercial routers and switches into a Humvee, a ship, or a plane and then sending those vehicles into the field. Rather, Network Centric Warfare is a powerful tool that directly brings to the warfighter important capabilities such as:

- Shared awareness to keep all warfighters fully informed, regardless of where they are in the battlespace
- Collaboration to help our distributed units fight together cohesively and cooperatively
- Synchronization to control the timing of our operations so as to magnify our striking power
- Understanding of Network Centric Warfare will expand the understanding of commanders at every level, so that each can make the right decision at the right time.

When DoD truly achieves the full capability that Network Centric Warfare has to offer, the network will be as important to the warfighter as any other weapon system on the battlefield. The ATO presentations that you will hear today will illustrate some of our ideas on how to make this happen.

Networks and their underlying communications capabilities have played an interesting and crucial role in military history. Over the past several centuries, we have seen military networks, their underlying technologies, and the use of these networks evolve into two separate camps.

On the one hand we have the enterprise side, where the national authorities and the warplanners operate. These are the folks who authorize, command, and coordinate large troop movements around the world. They have support teams that have specialized in administering large scale logistics, and in providing high level authorities the

intelligence products they need to make far-reaching decisions.

At the other extreme, we have the tactical edge. This is the front line where our troops are, right now, engaging the enemy. Out at the pointy end of the spear, these are the folks who find out every day whether or not we have delivered the capabilities they need. Our warfighters live in an increasingly mobile world, one in which there is no fixed infrastructure for them to use.

The history of warfare is a story of these two camps proceeding on two separate development paths. They have developed different networks, different communications gear, and different ways of doing business. As a result, important information that could have transformed our warfighting efforts, whether it was augmenting our striking power or averting strategic disaster, has all-too-often been proprietary to one camp or the other.

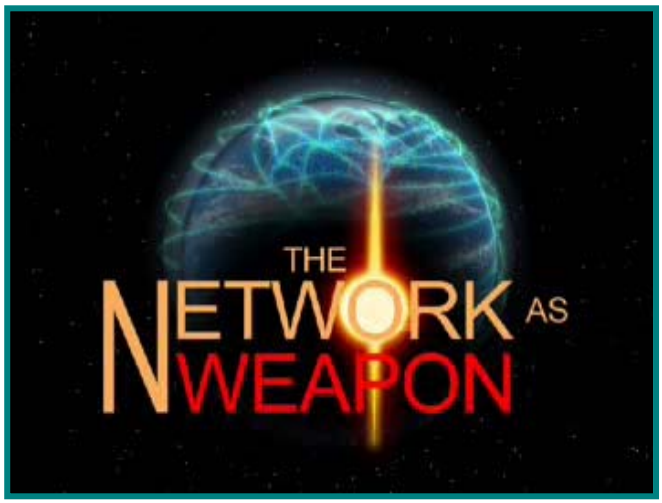
Today, that is changing. For the first time, we have an opportunity to bring these two camps together, linking them in a way that provides intelligence and insight seamlessly throughout our warfighting network.

When that happens, the Network becomes more than just a means of communication, the network becomes a weapon. Transforming the network from a weapons support system into a weapon itself, that is the thread that runs through the programs that we pursue. This is the problem ATO is working to solve.

Warfighters have been asking us, "What does it mean to see the network as a weapon, as important as any other weapons we bring to the battlefield? How do we use networks to find the enemy and to carry the fight to him?"

DARPA has answered these questions with earlier programs like Small Unit Operations Situation

The Network as Weapon



Awareness System (SUO-SAS), which demonstrated DoD's first tactical level, self-forming, radio network, and has since transitioned to the Army as the Soldier Radio Waveform in the Joint Tactical Radio System (JTRS), and WolfPack, our distributed, autonomous, unattended electronic warfare sensor network, capable of SIGINT, geo-location, and even jamming operations. Late last year, WolfPack was fielded as part of the Navy and Special Forces SILENT HAMMER exercise, demonstrating its value in threat detection, identification, and neutralization.

In our FCS Communications program, we have put in the hands of the warfighter a new and highly effective tool for synchronizing combat operations.

We've been demonstrating the value of the network at the application layer as well with the Command Post of the Future. This has become the Command Post of the present, right now in Iraq. This program brings innovative sharing and collaboration tools to the warfighters, and enables them to employ truly adaptive tactics and operations in the field.

Finally, not only does ATO make the things that make networks work, but we also partner with our Armed Services to understand how networks can be adapted to modern combat.

At the last DARPATech, we told you about our Maritime program, and showed how networks could enhance our ability to operate in the challenging littoral environment. This year, we'll highlight our efforts to apply networks to enable the Marines to mount fully distributed operations. Our goal is to use networks to help small teams in different corners of the battlefield communicate, survey the situation, and, when necessary, swarm to defend a unit under attack or overwhelm an enemy.

So, what are the challenges we face as we transform the network into a weapon? Start with the challenge of connectivity, because, without question, the level and sophistication that's coming is far beyond the capabilities of today's Global Information Grid. What this means for responsiveness and global reach dwarfs everything that's come before.

So too does the challenge of creating an effective network of networks that guarantees continuity of communications across network boundaries. It means learning how to embrace the diversity of the communications systems we see in the real world, and finding ways to stitch dissimilar networks into a seamless, heterogeneous whole.

At the edge of the Net, we face even tougher technical challenges. There are no cell towers to connect with, no infrastructure in place waiting for the warfighter to tap into. This is a rapidly mobile environment where RF signals don't propagate well and US forces don't have the freedom to reposition just to establish communications links. We have to provide our tactical forces a degree of robust and secure interconnectivity that exceeds anything we will ever find in the commercial sector.

And, we must enable the network to defend itself against those adversaries who seek to deny us the use of this valuable combat resource. We must develop network technologies that are robust enough to withstand attacks by the most determined adversaries, and that continue to deliver the services that the warfighter needs at all times.

The final challenges we face are:

- What will we do with that connectivity?

The Network as Weapon

- How will we use it to increase warfighting productivity?

After all, it's what the networked warfighter can do with his connectivity, and how it impacts the enemy, that defines mission success.

Those of you who remember the early days of the Internet and ARPAnet know that there was quite a time lag between when we established the connectivity and when we finally had useful applications like web browsers, net meetings, and other collaboration tools.

The reason for this time lag wasn't a failure of innovation, it was a failure of imagination, the ability to think forward into a new future. To truly gain an advantage with new technology, we must overcome this inability to think forward into a new place, define a new paradigm and its new potential.

In the case of Network Centric Warfare, there is no commercial parallel, there are no off-the-shelf clues. We need to envision how to use the high-bandwidth connectivity that future military networks will provide and we need to do it now, not 10 to 15 years after the capability exists.

During the rest of the ATO presentations, you'll hear what we're doing in ATO to create that leap-ahead potential, work that we believe puts us at the cutting edge of the connectivity race.

First, we will start with two backbone technologies critical to the network as weapon.

- Adel Saleh will take us through novel approaches for enterprise networks
- Preston Marshall will speak about the mobile, tactical side
- Next, you'll hear about three different tactical applications:
- Ryan Patterson will focus on the Command Post of the Future, a tool that is transforming the way our forces operate in Iraq
- Khine Latt will follow with the technologies that will help secure naval superiority
- Ed Tovar will tell you about the Distributed Operations Program, a real test for Network Centric Warfare

Having seen how important Network Centric Warfare is to our warfighters, you will then hear from Anup Ghosh about the defense of our networks, by definition, the network as weapon becomes a target. Therefore, defending our network is paramount. Finally, Larry Stotts will wrap up this session and show how you can help us achieve this ATO vision.

So, as I said at the outset, we are inventing the future in ATO, and making Network Centric Warfare the key to DoD dominating future military operations. In the conflicts of the future, the DoD network will be just as important as any other weapon system, and therefore needs to be planned, developed, and defended as rigorously as any other weapon system.